From: SANS AtRisk
To: ndaigle@bakersfieldpd.us
Subject: @RISK: The Consensus Security Vulnerability Alert: Vol. 19, Num. 21
Date: Thursday, May 23, 2019 5:01:16 AM
Attachments: smime.p7s

@RISK: The Consensus Security Vulnerability Alert
May 23, 2019 - Vol. 19, Num. 21

Providing a reliable, weekly summary of newly discovered attack vectors, vulnerabilities with active exploits, and explanations of how recent attacks worked

Archived issues may be found at http://www.sans.org/newsletters/at-risk

---

CONTENTS:

- NOTABLE RECENT SECURITY ISSUES
- INTERESTING NEWS FROM AROUND THE SECURITY COMMUNITY
- VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE
- MOST PREVALENT MALWARE FILES May 16 -23, 2019

TOP VULNERABILITY THIS WEEK: Microsoft warns of wormable remote code execution bug

---

********** **Sponsored By ExtraHop** **********

Don't miss: ***How To Increase MITRE ATT&CK Coverage with Network Traffic Analysis.*** In this presentation you'll learn how to take your ATT&CK understanding and coverage to the next level with network traffic analysis.

Register: **http://www.sans.org/info/212875**

TRAINING UPDATE

SANSFIRE 2019 | Washington, DC | June 15-22

SANS Kansas City 2019 | June 10-15

Security Operations Summit 2019 | New Orleans, LA | June 24-July 1

SANS Charlotte 2019 | July 8-13

SANS Pittsburgh 2019 | July 8-13

SANS Columbia 2019 | Columbia, MD | July 15-20

SANS Rocky Mountain 2019 | Denver, CO | July 15-20

SANS San Francisco Summer 2019 | July 22-27

DFIR Summit & Training 2019 | Austin, TX | July 25-August 1

SANS Cyber Defence Canberra 2019 | June 24-July 13

SANS London July 2019 | July 8-13

SANS OnDemand and vLive Training
Get a Free GIAC Certification Attempt or Take $350 Off your OnDemand or vLive course. Offer ends May 29.

Single Course Training
SANS Mentor and Community SANS

View the full SANS course catalog and skills roadmap

Sponsored Links:

ICYMI: ***New Year, Same Magecart: The Continuation of Web-based Supply Chain Attacks.*** Get it here: **http://www.sans.org/info/212880**

Don't miss ***Streamlining Your Security Process with Orchestration & Automation*** with Lauren Taylor and Jadon Montero. Register: **http://www.sans.org/info/212885**

ICYMI: ***Increasing Visibility with Ixia's Vision ONE*** with Serge Borso and Taran Singh. Register: **http://www.sans.org/info/212890**

NOTABLE RECENT SECURITY ISSUES
SELECTED BY THE TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Title: **Coverage available for critical vulnerability in Microsoft Remote Desktop Protocol**
Description: Microsoft continues to urge users to update to the latest version of the Remote Desktop Protocol to patch a wormable remote code execution bug. The vulnerability opens up victims to an attack where malware spreads from one machine to another once this bug is exploited only once. The company disclosed this vulnerability last week as part of its monthly security update. The company disclosed this vulnerability as CVE-2019-0708 last week as part of its monthly security update.
Reference: **https://www.csoonline.com/article/3395444/microsoft-urges-windows-customers-to-patch-wormable-rdp-flaw.html**
Snort SIDs: 50137

Title: **Multiple vulnerabilities in Wacom Update Helper**
Description: There are two privilege escalation vulnerabilities in the Wacom update helper. The update helper is a utility installed alongside the macOS application for Wacom tablets. The application interacts with the tablet and allows the user to manage it. These vulnerabilities could allow an attacker with local access to raise their privileges to root.
Reference: **https://blog.talosintelligence.com/2019/05/wacom-update-helper-vuln-spotlight-may-2019.html**
Snort SIDs: 48850, 48851

INTERESTING NEWS FROM AROUND THE SECURITY COMMUNITY

The U.S. Department of Homeland Security sent out a warning that some Chinese-made drones may be transmitting sensitive data back to their manufacturers.
https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html

A popular forum for people involved in stealing online accounts and carrying out SIM-swapping attacks was hacked, exposing the hashed passwords, IP addresses, email addresses and private users for more than 110,000 of its members.
https://krebsonsecurity.com/2019/05/account-hijacking-forum-ogusers-hacked/

The MuddyWater APT recently made some changes to its well-known BlackWater malware that make it more difficult to detect and easier for it to establish persistence.
https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html

Cisco has released firmware updates to address a critical flaw in its Secure Boot implementation; while fixes are currently available for some products, patches for others will not be available until later this year.
https://threatpost.com/cisco-patch-firmware/144936/

A misconfiguration in some of the most popular Docker containers could open them to attack; the issue affects containers from Microsoft, Monsanto and the British government.
https://www.zdnet.com/article/root-account-misconfigurations-found-in-20-of-top-1000-docker-containers/

San Francisco passed a law banning the government's use of facial recognition technology, which is expected to set up battles in other cities and states between law enforcement officials and privacy advocates.
https://www.nbcnews.com/news/us-news/san-francisco-s-facial-recognition-ban-just-beginning-national-battle-n1007186

RECENT VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE
COMPILED BY THE QUALYS VULNERABILITY RESEARCH TEAM

This is a list of recent vulnerabilities for which exploits are available. System administrators can use this list to help in prioritization of their remediation activities. The Qualys Vulnerability Research Team compiles this information based on various exploit frameworks, exploit databases, exploit kits and monitoring of internet activity.

ID: CVE-2019-1727
Title: **Cisco NX-OS Software Local Privilege Escalation Vulnerability**
Vendor: Cisco
Description: Cisco NX-OS Software for Nexus Series Switches is exposed to a local privilege escalation vulnerability. Local attackers may exploit this issue to gain elevated privileges. A vulnerability in the Python scripting subsystem of Cisco NX-OS Software could allow an authenticated, local attacker to escape the Python parser and issue arbitrary commands to elevate the attacker's privilege level. The vulnerability is due to insufficient sanitization of user-supplied parameters that are passed to certain Python functions in the scripting sandbox of the affected device. An attacker could exploit this vulnerability to escape the scripting sandbox and execute arbitrary commands to elevate the attacker's privilege level.
CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-1806
Title: **Cisco Small Business Series Switches Denial of Service Vulnerability**
Vendor: Cisco
Description: Cisco Small Business Series Switches are exposed to a remote denial ofservice vulnerability. An attacker can exploit this issue to cause denial of service conditions. A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco Small Business Sx200, Sx300, Sx500, ESW2 Series Managed Switches and Small Business Sx250, Sx350, Sx550 Series Switches could allow an authenticated, remote attacker to cause the SNMP application of an affected device to cease processing traffic, resulting in the CPU utilization reaching one hundred percent. Manual intervention may be required before a device resumes normal operations. The vulnerability is due to improper validation of SNMP protocol data units (PDUs) in SNMP packets. An attacker could exploit this vulnerability by sending a malicious SNMP packet to an affected device. A successful exploit could allow the attacker to cause the device to cease forwarding traffic, which could result in a denial of service condition.
CVSS v2 Base Score: 6.8 (AV:N/AC:L/Au:S/C:N/I:N/A:C)

ID: CVE-2017-14491
Title: **Dnsmasq Multiple Security Vulnerabilities**
Vendor: Thekelleys
Description: Dnsmasq is prone to multiple security vulnerabilities. Attackers can exploit these issues to execute arbitrary code within the context of the affected application, bypass the ASLR or gain sensitive information, or cause a denial of service condition. Heap-based buffer overflow in dnsmasq allows remote attackers to cause a denial of service or execute arbitrary code via a crafted DNS response.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2015-5504
Title: **Drupal Novalnet Payment Module- Ubercart Module SQL Injection Vulnerability**
Vendor: Drupal
Description: The Novalnet Payment Module Ubercart Module for Drupal is exposed to a SQL injection vulnerability because it fails to sufficiently sanitize user supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. SQL injection vulnerability in the Novalnet Payment Module Ubercart module for Drupal allows remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-11205
Title: **Multiple TIBCO Products Multiple Unspecified Cross-Site Scripting Vulnerabilities**
Vendor: Tibco
Description: Multiple TIBCO Products are exposed to multiple unspecified cross site scripting vulnerabilities because it fails to properly sanitize user-supplied input. An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and to launch other attacks. The web server component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and TIBCO Spotfire Server contains vulnerabilities that theoretically allow reflected cross-site scripting attacks.
CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

ID: CVE-2019-11328
Title: **Singularity Insecure Permissions Local Privilege Escalation Vulnerability**
Vendor: Sylabs
Description: Singularity is exposed to a local privilegeescalation vulnerability. Local attackers can exploit this issue to gain elevated privileges on affected computers. An malicious user with local/network access to the host system (e.g. ssh) could exploit this vulnerability due to insecure permissions allowing a user to edit files within

`/run/singularity/instances/sing/<user>/<instance>`. The manipulation of those files can change the behavior of the starter-suid program when instances are joined resulting in potential privilege escalation on the host.
CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

ID: CVE-2019-10139
Title: **cockpit-ovirt Local Information Disclosure Vulnerability**
Vendor: oVirt
Description: cockpit-ovirt is prone to local information-disclosure vulnerability.
An attacker can exploit this issue to gain access to sensitive information; this may lead to further attacks.
During HE deployment via cockpit-ovirt, cockpit-ovirt generates an ansible variable file `/var/lib/ovirt-hosted-engine-setup/cockpit/ansibleVarFileXXXXXX.var` which contains the admin and the appliance passwords as plain-text. At the of the deployment procedure, these files are deleted.
CVSS v2 Base Score: 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

ID: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091
Title: **Intel Processor MDS Vulnerabilities**
Vendor: Intel
Description: Modern Intel microprocessors implement hardware level micro optimizations to improve the performance of writing data back to CPU caches. These vulnerabilities are collectively referred as Microarchitectural Data Sampling issues (MDS issues) because they refer to issues related to microarchitectural structures of the Intel processors other than the level 1 data cache. The affected microarchitectural structures in the affected Intel processors are the Data Sampling Uncacheable Memory (uncacheable memory on some microprocessors utilizing speculative execution), the store buffers (temporary buffers to hold store addresses and data), the fill buffers (temporary buffers between CPU caches), and the load ports (temporary buffers used when loading data into registers). As a result of the flaw in the architecture of these processors, an attacker who can execute malicious code locally on an affected system can compromise the confidentiality of data previously handled on the same thread or compromise the confidentiality of data from other hyperthreads on the same processor as the thread where the malicious code executes.
CVSS v2 Base Score: 4.9 (AV:L/AC:L/Au:N/C:C/I:N/A:N)

MOST PREVALENT MALWARE FILES May 16 - 23, 2019
COMPILED BY TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

SHA 256: 3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3
MD5: 47b97de62ae8b2b927542aa5d7f3c858
VirusTotal:
https://www.virustotal.com/#/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details
Typical Filename: qmreportupload.exe
Claimed Product: qmreportupload
Detection Name: Win.Trojan.Generic::in10.talos

SHA 256: 6dfaacd6f16cb86923f21217ca436b09348ee72b34849921fed2a17bddd59310
MD5: 7054c32d4a21ae2d893a1c1994039050
VirusTotal:
https://www.virustotal.com/#/file/6dfaacd6f16cb86923f21217ca436b09348ee72b34849921fed2a17bddd59310/details
Typical Filename: maftask.zip
Claimed Product: N/A
Detection Name: PUA.Osx.Adware.Advancedmaccleaner::tpd

SHA 256: 15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b
MD5: 799b30f47060ca05d80ece53866e01cc
VirusTotal:
https://www.virustotal.com/#/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details
Typical Filename: 15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b.bin
Claimed Product: N/A
Detection Name: W32.Generic:Gen.22fz.1201

SHA 256: c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f
MD5: e2ea315d9a83e7577053f52c974f6a5a
VirusTotal:
https://www.virustotal.com/#/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details
Typical Filename: Tempmf582901854.exe
Claimed Product: N/A
Detection Name: W32.AgentWDCR:Gen.21gn.1201

SHA 256: 7acf71afa895df5358b0ede2d71128634bfbbc0e2d9deccff5c5eaa25e6f5510

MD5: 4a50780ddb3db16ebab57b0ca42da0fb
VirusTotal:
https://www.virustotal.com/#/file/7acf71afa895df5358b0ede2d71128634bfbbc0e2d9deccff5c5eaa25e6f5510/details
Typical Filename: wup.exe
Claimed Product: N/A
Detection Name: W32.7ACF71AFA8-95.SBX.TG

(c) 2019. All rights reserved. The information contained in this newsletter, including any external links, is provided "AS IS," with no express or implied warranty, for informational purposes only.

Please feel free to share this with interested parties via email, but no posting is allowed on web sites. For a free subscription visit https://www.sans.org/account/create

SANS Institute Privacy Policy
11200 Rockville Pike, Suite 200, North Bethesda, MD, 20852

To change your email address visit update profile.
To change your email preferences or unsubscribe visit manage subscriptions.

This mailbox is not monitored. Please email support@sans.org or call 301-654-7267 for assistance.